Chapter 3
System Analysis
Fault Tree Analysis

Marvin Rausand
Department of Production and Quality Engineering
Norwegian University of Science and Technology
marvin.rausand@ntnu.no

Introduction

What is fault tree analysis?

- Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a potential undesirable event (accident) called a TOP event, and then determining all the ways it can happen.
- The analysis proceeds by determining how the TOP event can be caused by individual or combined lower level failures or events.
- The causes of the TOP event are "connected" through logic gates
- In this book we only consider AND-gates and OR-gates
- FTA is the most commonly used technique for causal analysis in risk and reliability studies.

History

- FTA was first used by Bell Telephone Laboratories in connection with the safety analysis of the Minuteman missile launch control system in 1962
- Technique improved by Boeing Company
- Extensively used and extended during the Reactor safety study (WASH 1400)

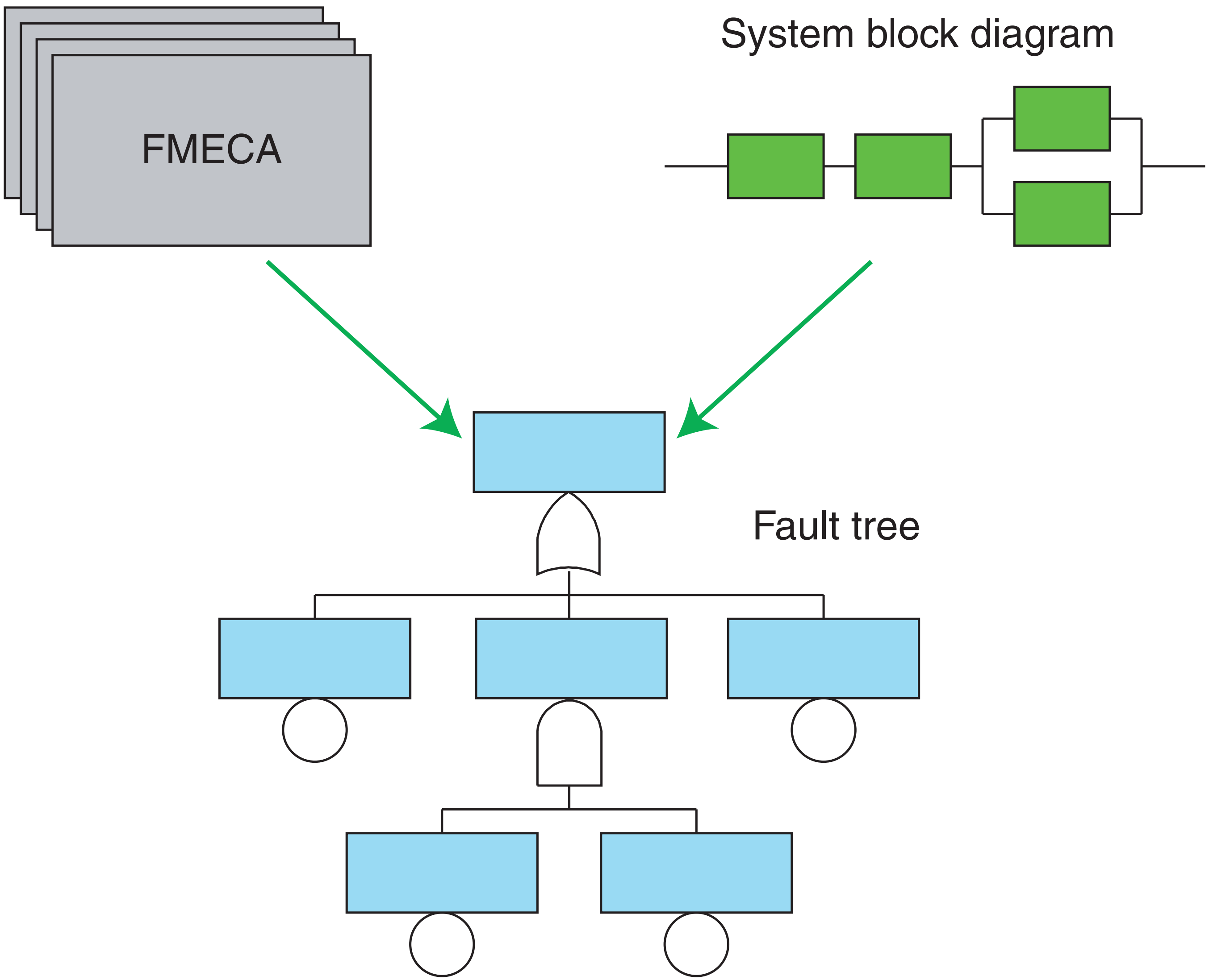
FTA main steps

- Definition of the system, the TOP event (the potential accident), and the boundary conditions
- Construction of the fault tree
- Identification of the minimal cut sets
- Qualitative analysis of the fault tree
- Quantitative analysis of the fault tree
- Reporting of results

Preparation for FTA

- The starting point of an FTA is often an existing FMECA and a system block diagram
- The FMECA is an essential first step in understanding the system
- The design, operation, and environment of the system must be evaluated
- The cause and effect relationships leading to the TOP event must be identified and understood

Preparation for FTA



Boundary conditions

- The physical boundaries of the system (Which parts of the system are included in the analysis, and which parts are not?)

- The initial conditions (What is the operational stat of the system when the TOP event is occurring?)
- Boundary conditions with respect to external stresses (What type of external stresses should be included in the analysis – war, sabotage, earthquake, lightning, etc?)
- The level of resolution (How detailed should the analysis be?)

Fault tree construction

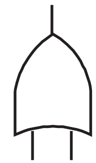
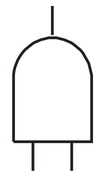
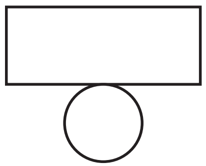
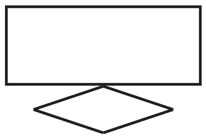
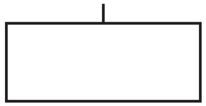
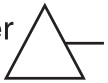
Fault tree construction

- Define the TOP event in a clear and unambiguous way. Should always answer:

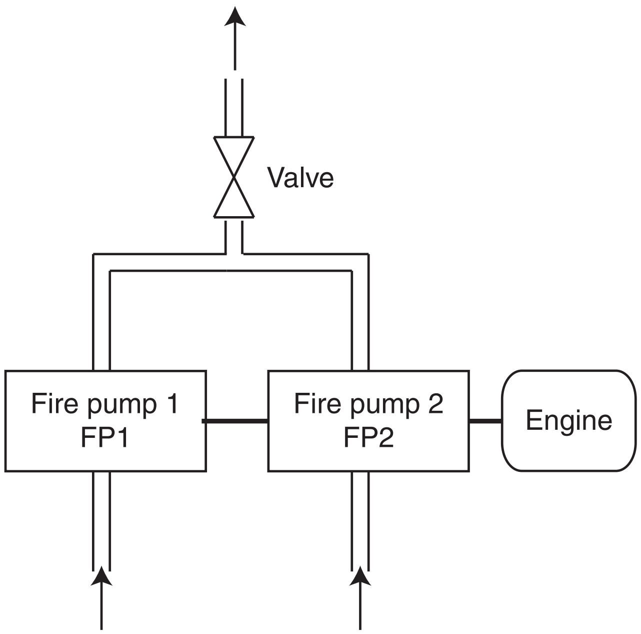
  What e.g., "Fire"
  Where e.g., "in the process oxidation reactor"
  When e.g., "during normal operation"

- What are the immediate, necessary, and sufficient events and conditions causing the TOP event?
- Connect via AND- or OR-gate
- Proceed in this way to an appropriate level (= basic events)
- Appropriate level:
  - Independent basic events
  - Events for which we have failure data

Fault tree symbols

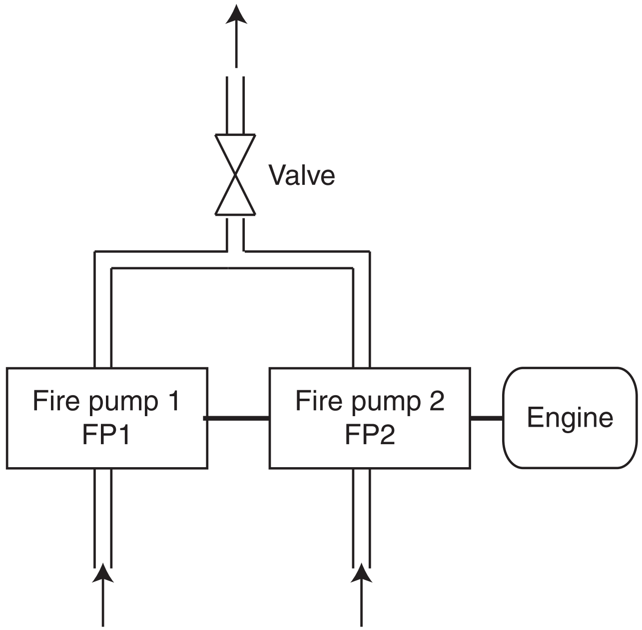
Logic gates	 OR-gate	The OR-gate indicates that the output event occurs if any of the input events occur
	 AND-gate	The AND-gate indicates that the output event occurs only if all the input events occur at the same time
Input events (states)		The basic event represents a basic equipment failure that requires no further development of failure causes
		The undeveloped event represents an event that is not examined further because information is unavailable or because its consequences are insignificant
Description of state		The comment rectangle is for supplementary information
Transfer symbols	Transfer out  Transfer in 	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol

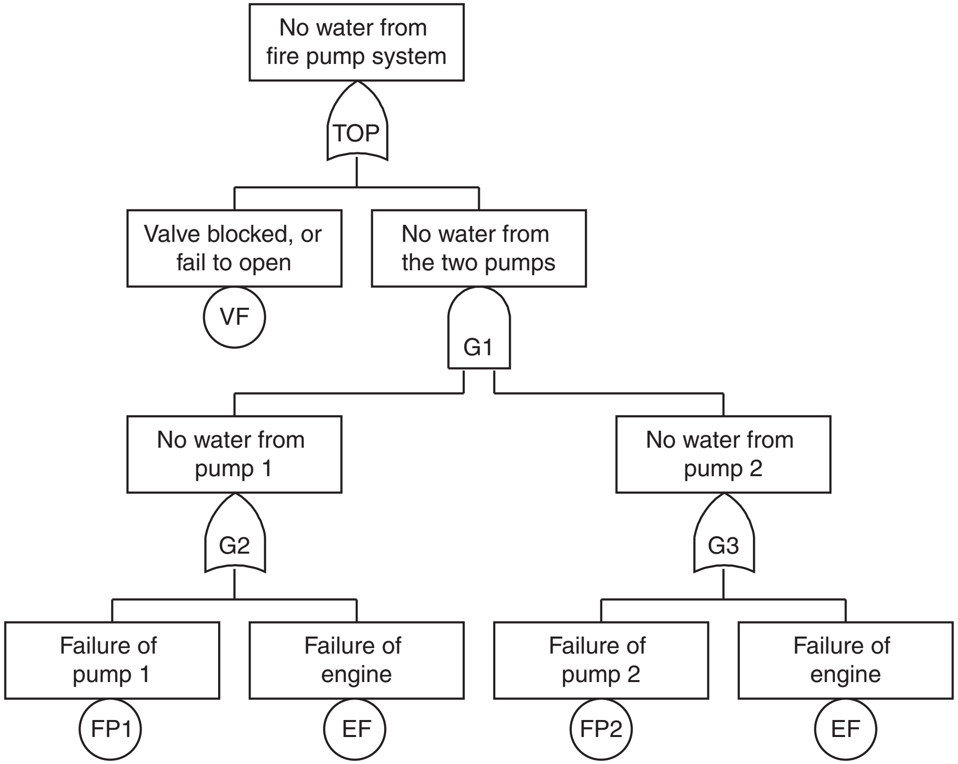
Example: Redundant fire pumps



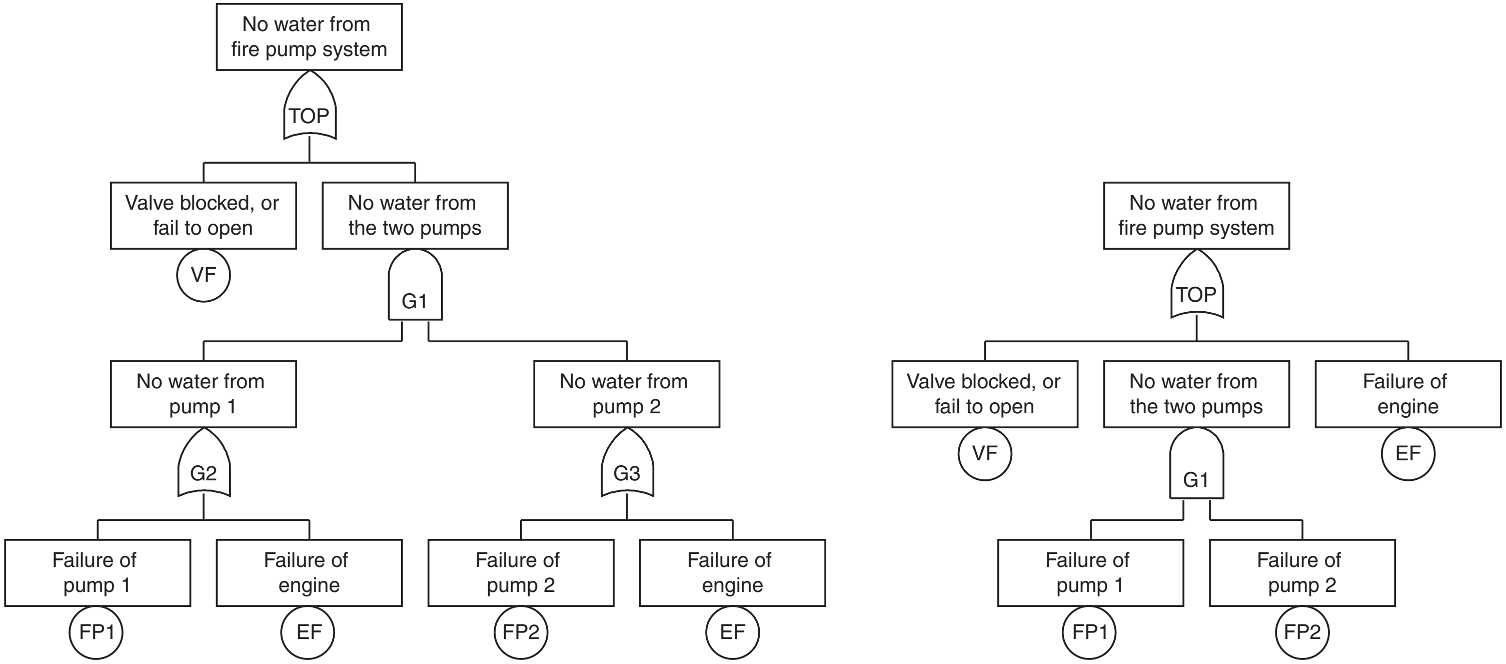
TOP event = No water from fire water system
Causes for TOP event:
VF = Valve failure
G1 = No output from any of the fire pumps
G2 = No water from FP1 G3 = No water from FP2
FP1 = failure of FP1
EF = Failure of engine
FP2 = Failure of FP2

Example: Redundant fire pumps (2)





Example: Redundant fire pumps (3)



The two fault trees above are logically identical. They give the same information.

Qualitative assessment

Cut Sets

- A *cut set* in a fault tree is a set of basic events whose (simultaneous) occurrence ensures that the TOP event occurs
- A cut set is said to be *minimal* if the set cannot be reduced without loosing its status as a cut set

The TOP event will therefore occur if all the basic events in a minimal cut set occur at the same time.

Qualitative assessment

Qualitative assessment by investigating the minimal cut sets:

- Order of the cut sets
- Ranking based on the type of basic events involved
    1. Human error (most critical)
    2. Failure of active equipment
    3. Failure of passive equipment
- Also look for "large" cut sets with dependent items

Rank	Basic event 1	Basic event 2
1	Human error	Human error
2	Human error	Failure of active unit
3	Human error	Failure of passive unit
4	Failure of active unit	Failure of active unit
5	Failure of active unit	Failure of passive unit
6	Failure of passive unit	Failure of passive unit

Quantitative assessment

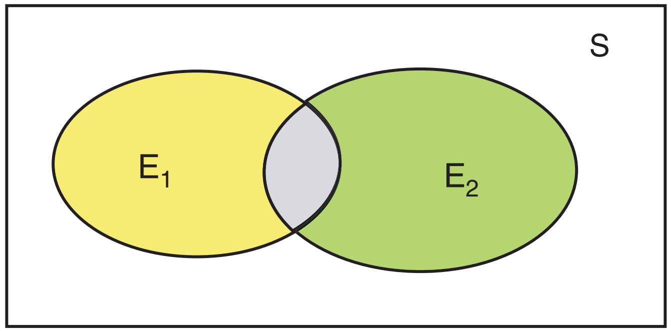
Notation

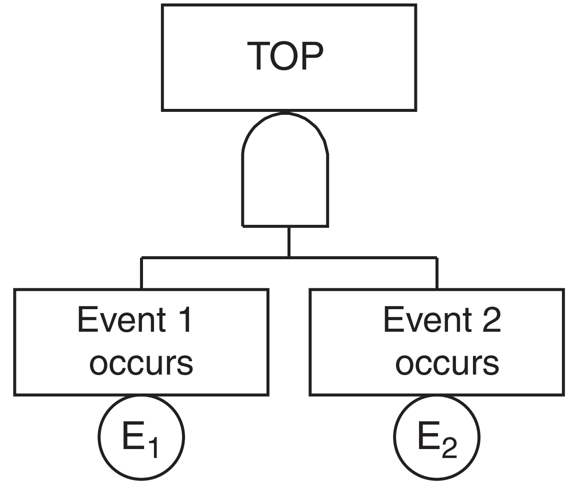
$$
\begin{aligned}
Q_0(t) &= \Pr(\text{The TOP event occurs at time } t) \\
q_i(t) &= \Pr(\text{Basic event } i \text{ occurs at time } t) \\
\check{Q}_j(t) &= \Pr(\text{Minimal cut set } j \text{ fails at time } t)
\end{aligned}
$$

- Let $E_i(t)$ denote that basic event i occurs at time t. $E_i(t)$ may, for example, be that component i is in a failed state at time t. Note that $E_i(t)$ does not mean that component i fails exactly at time t, but that component i is in a failed *state* at time t
- A minimal cut set is said to fail when all the basic events occur (are present) at the same time.

The formulas for $q_i(t)$ will be discussed later in this presentation.

Single AND-gate





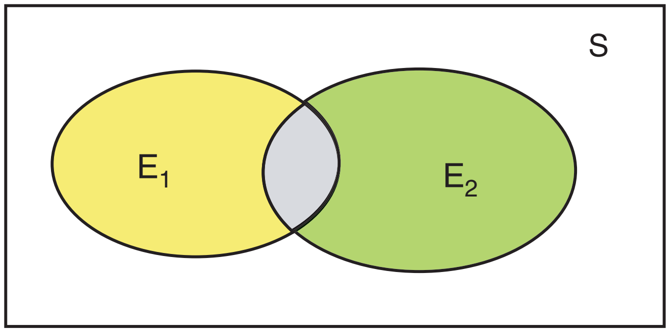
Let $E_i(t)$ denote that event E_i occurs at time t, and let $q_i(t) = \Pr(E_i(t))$ for $i = 1, 2$. When the basic events are independent, the TOP event probability $Q_0(t)$ is

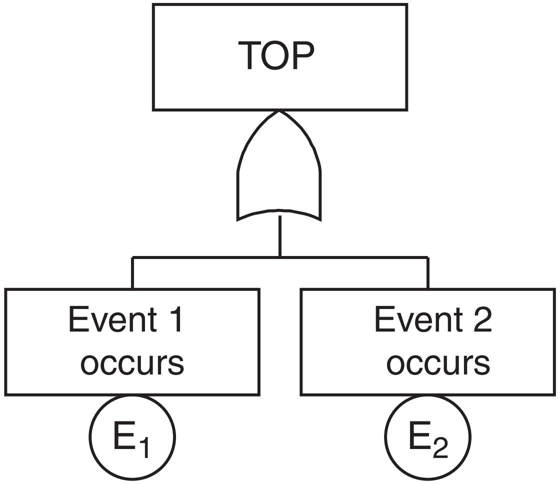
$$Q_0(t) = \Pr(E_1(t) \cap E_2(t)) = \Pr(E_1(t)) \cdot \Pr(E_2(t)) = q_1(t) \cdot q_2(t)$$

When we have a single AND-gate with m basic events, we get

$$Q_0(t) = \prod_{j=1}^{m} q_j(t)$$

Single OR-gate





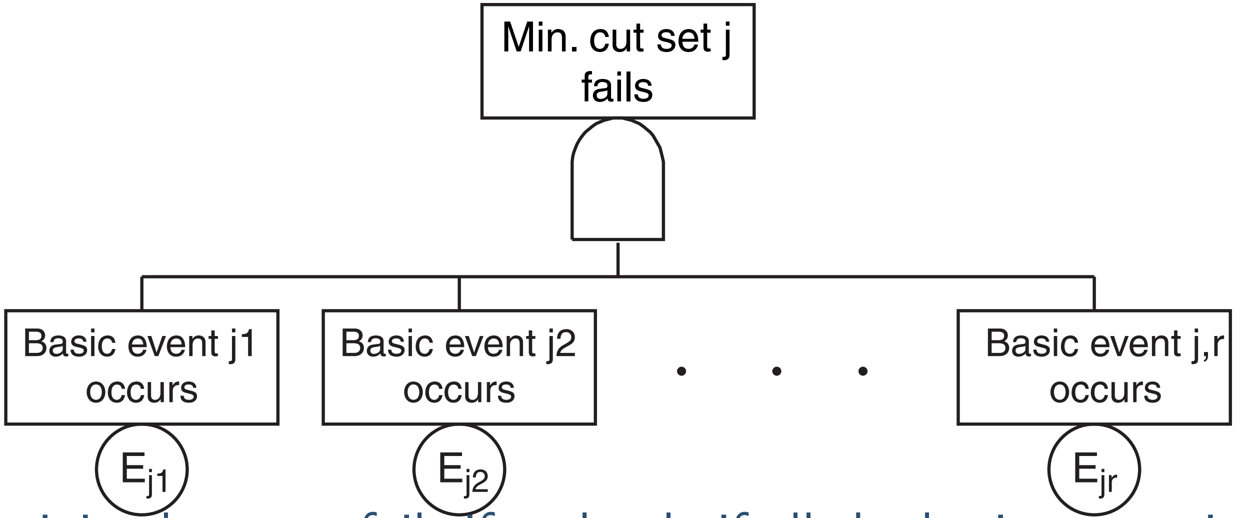
When the basic events are independent, the TOP event probability $Q_0(t)$ is

$$\begin{aligned} Q_0(t) &= \Pr(E_1(t) \cup E_2(t)) = \Pr(E_1(t)) + \Pr(E_2(t)) - \Pr(E_1(t) \cap E_2(t \\ &= q_1(t) + q_2(t) - q_1(t) \cdot q_2(t) = 1 - (1 - q_1(t))(1 - q_2(t)) \end{aligned}$$

When we have a single OR-gate with m basic events, we get

$$Q_0(t) = 1 - \prod_{j=1}^{m} (1 - q_j(t))$$

Cut set assessment

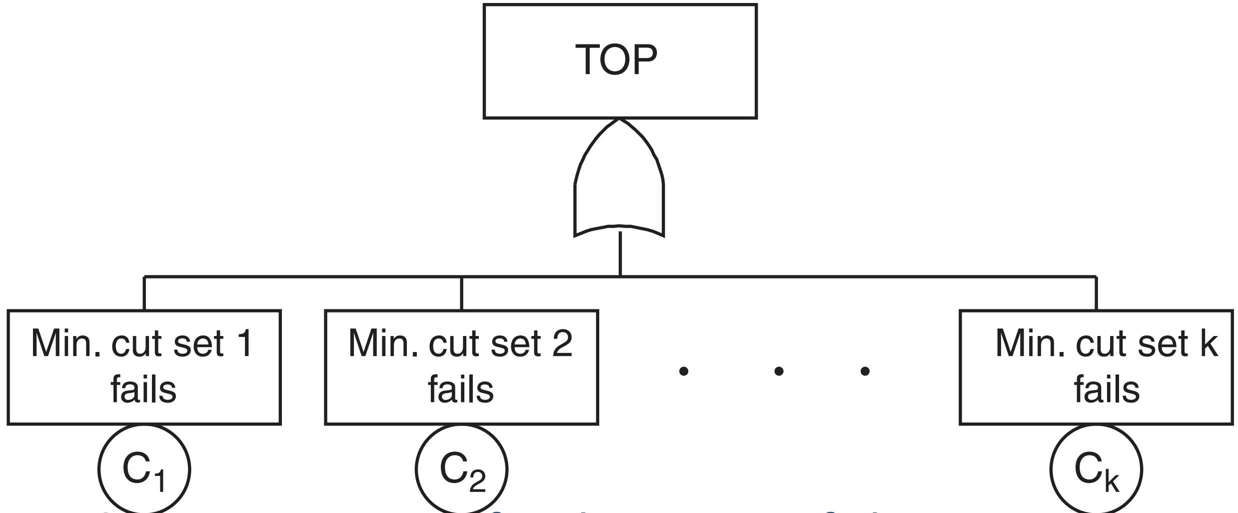


A minimal cut set fails if and only if all the basic events in the set fail at the same time. The probability that cut set j fails at time t is

$$\check{Q}_j(t) = \prod_{i=1}^{r} q_{j,i}(t)$$

where we assume that all the r basic events in the minimal cut set j are independent.

TOP event probability



The TOP event occurs if at least one of the minimal cut sets fails. The TOP event probability is

$$Q_0(t) \leq 1 - \prod_{j=1}^{k} \left(1 - \check{Q}_j(t)\right) \tag{1}$$

The reason for the inequality sign is that the minimal cut sets are not always independent. The same basic event may be member of several cut sets. Formula (1) is called the *Upper Bound Approximation*.

Input Data

Types of events

Five different types of events are normally used:

- Non-repairable unit
- Repairable unit (repaired when failure occurs)
- Periodically tested unit (hidden failures)
- Frequency of events
- On demand probability

Basic event probability:

$$q_i(t) = \Pr(\text{Basic event } i \text{ occurs at time } t)$$

Non-repairable unit

Unit i is not repaired when a failure occurs.

Input data:

- Failure rate λ_i

Basic event probability:

$$q_i(t) = 1 - e^{-\lambda_i t} \approx \lambda_i t$$

Repairable unit

Unit i is repaired when a failure occurs. The unit is assumed to be “as good as new” after a repair.

Input data:

- Failure rate λ_i
- Mean time to repair, MTTR_i

Basic event probability:

$$q_i(t) \approx \lambda_i \cdot \text{MTTR}_i$$

Periodic testing

Unit i is tested periodically with test interval τ. A failure may occur at any time in the test interval, but the failure is only detected in a test or if a demand for the unit occurs. After a test/repair, the unit is assumed to be "as good as new".
This is a typical situation for many safety-critical units, like sensors, and safety valves.

Input data:

- Failure rate λ_i
- Test interval τ_i

Basic event probability:

$$q_i(t) \approx \frac{\lambda_i \cdot \tau_i}{2}$$

Frequency

Event i occurs now and then, with no specific duration

Input data:

- Frequency f_i
- If the event has a duration, use input similar to repairable unit.

On demand probability

Unit i is not active during normal operation, but may be subject to one or more demands

Input data:

- $\mathrm{Pr}($Unit i fails upon request$)$
- This is often used to model operator errors.

Cut set evaluation

Ranking of minimal cut sets:

- Cut set unavailability
  The probability that a specific cut set is in a failed state at time t
- Cut set importance
  The conditional probability that a cut set is failed at time t, given that the system is failed at time t

Conclusions

- FTA identifies all the possible causes of a specified undesired event (TOP event)
- FTA is a structured top-down deductive analysis.
- FTA leads to improved understanding of system characteristics. Design flaws and insufficient operational and maintenance procedures may be revealed and corrected during the fault tree construction.
- FTA is not (fully) suitable for modelling dynamic scenarios
- FTA is binary (fail–success) and may therefore fail to address some problems